UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/457,732	12/10/1999	ANDREA CALIFANO	YO999-137	8003

21254 7590 01/04/2010

MCGINN INTELLECTUAL PROPERTY LAW GROUP, PLLC
8321 OLD COURTHOUSE ROAD
SUITE 200
VIENNA, VA 22182-3817

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2439	
MAIL DATE	DELIVERY MODE
01/04/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ANDREA CALIFANO,
STEPHEN CARL KAUFMAN,
MARCO MARTENS,
WILLIAM ROBERT PULLEYBLANK,
GUSTAVO ALEJANDRO STOLOVITZKY,
CHARLES PHILIPPE TRESSER,
and CHAI WAH WU

Appeal 2009-001001
Application 09/457,732
Technology Center 2400

Decided: December 31, 2009

Before HOWARD B. BLANKENSHIP, CAROLYN D. THOMAS, and STEPHEN C. SIU, *Administrative Patent Judges*.

BLANKENSHIP, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1, 5-9, and 11-36, which are all of the claims remaining in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm-in-part.

Invention

Appellants' invention relates to a method of processing biometric data by receiving a data set P, selecting a secure hash function h, computing h(P), destroying data set P, and storing h(P) in a data base. Abstract.

Representative Claim

1. A method of processing semiotic data, comprising:

receiving semiotic data including at least one data set P;

selecting a function h, and for at least one of each said data set P to be collected, computing h(P);

destroying said data set P;

storing h(P) in a database, and

obtaining a sample of P' such that a comparison can be made;

at least one of obtaining and computing h(P'); and

to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P,

wherein said data set P cannot be extracted from h(P),

wherein said semiotic data comprises biometric data,

wherein said function h comprises a secure hash function,

wherein the data set P is not determined perfectly by its reading,

wherein each reading gives a number Pi, wherein i is no less than 0, wherein P0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof,

wherein reading P0 is different from Pi for $i > 0$, and the secret version of P0 is different from the secret version of Pi, such that no identification is possible by a direct comparison of the encrypted data,

said method further comprising:

extracting sub-collections Sj from the collection of data in data set P;

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability,

comparing encrypted versions of the sub-collections Sj with those data stored in said database,

wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred,

each time a Pi, with $i > 0$, is read, computing all possible predetermined size variations of Pi which correspond to an acceptable predetermined imprecision of the reading;

and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database,

wherein for a plurality of users of the same biometric information, said biometric information is encrypted differently for each user, and

wherein at least one of said data set P and P' comprises a personal data set.

Prior Art

Borza	U.S. 6,446,210 B1	Sep. 3, 2002
Kharon	U.S. 6,487,662 B1	Nov. 26, 2002

Alfred J. Menezes, et al., *Handbook of Applied Cryptography*, 321-375 (CRC Press, 1997).

Examiner's Rejections

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 101 as lacking utility.

Claims 31-36 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter.

Claims 1, 5-9, and 11-36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza and Kharon.

The Answer indicates that claims 9, 15, 17, 27, and 33 are rejected under 35 U.S.C. § 102(e). Ans. 11-12. However, the Final Rejection (at 13-17) and the Appellants' statement of the grounds of rejection (App. Br. 23) indicate that claims 9, 15, 17, 27, and 33 are rejected under 35 U.S.C. § 103(a). Further, the Answer (at 2) says that Appellants' statement of the

grounds of rejection in the Appeal Brief is correct. In any event, the Answer's new ground of rejection for claims 9, 15, 17, 27, and 33 under 35 U.S.C. § 102(e) has not been approved by a director or designee of the Technology Center. *See* MPEP § 1207.03. We conclude that the grounds of rejection set forth in the Final Rejection are the grounds for review in this appeal.[1]

ISSUES

(1) Have Appellants shown that the Examiner erred in finding that the invention recited in claims 1, 14-16, 31, and 32 lacks utility?

(2) Have Appellants shown that the Examiner erred in finding that claims 31-36 are directed to a transitory, propagating signal?

(3) Have Appellants shown that the Examiner erred in finding that the combination of Borza and Kharon teaches "to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P" and "encrypting a predetermined number of such sub-collections" as recited in claim 1?

---

[1] The Examiner attempted to "correct" the errors in the Answer by later mailing a paper that asserted the Answer should state that all the claims are rejected under § 103(a). However, the Answer does not set forth § 103 rejections for the claims listed in the new rejection. Nor does the later paper withdraw the § 102 rejection of the claims that was set forth in the Answer. In any event, Appellants had the opportunity to file a petition contesting entry of the Answer, or to complain in the Reply Brief. Appellants did neither, and have thus waived any arguments with respect to procedural errors that might have been created subsequent to the final rejection.

FINDINGS OF FACT

Borza

1. Encrypted characterised biometric information is compared against an encrypted template, which provides enhanced security for a variety of reasons. First, the actual templates need not be stored on the server, thereby preventing unauthorised access. Second, a destructive encryption algorithm may be employed to prevent decryption of the data. Destructive encryption algorithms are known in the art of computer security and are often used prior to storing or verifying user passwords. Col. 8, ll. 28-38.

2. The authentication procedure determines an independent sequence of comparison scores from the input provided by the candidate. This sequence is considered to be a point "P" in n-dimensional vector space. A threshold function is used to determine whether or not the point belongs to a set. The identity of the individual is confirmed if and only if the point belongs to the set. Col. 14, ll. 21-59.

3. Identification of an individual is performed by evaluating resulting values from the registration to determine a probability, for those results, of false acceptance and false rejection. When the value is within predetermined limits for an acceptable value, identification is provided. When the value falls outside the predetermined limits identification is not provided. Col. 16, ll. 31-37.

4. Identification of an individual is performed by evaluating resulting values from the registration to determine a quality of user identification. When the quality is within predetermined limits for an

acceptable quality, identification is provided. When the value falls outside the predetermined limits identification is not provided. Col. 16, ll. 52-58.

Kharon

5. The minutia extraction step 340 further proceeds with exclusion of minutia that are too closely located. Referring to FIG. 10, two end minutia at (x1, y1) and (x2, y2), respectively, and represented by vectors (p1,q1) and (p2,q2) respectively, are shown. First, determination is made as to whether the two minutia are within a threshold distance. This threshold distance is optionally a distance r used to determine matching minutia and as discussed below, is a fixed distance, or another distance based on mean ridge line separation distance. When two minutia are within the given threshold distance, a determination is made whether the angle between the two vectors (p1,q1) and (p2,q2) is within a given threshold of 180 degrees and the angle between (p2,q2) and (x2-x1, y2-y1) is within a given threshold of 0. If two minutia satisfy the aforesaid criteria they are excluded because they are too close and aligned in a nearly straight line. As a result of the minutia extraction process, the print image FP is now represented by a data set. The minutia extraction is advantageous in reducing the amount of data to be processed and thereby reducing the processing time and requirements. Col. 13, ll. 43-67.

PRINCIPLES OF LAW

Utility

If the claimed subject matter is inoperative, the invention fails to meet the utility requirement of 35 U.S.C. § 101. However, to violate § 101, the claimed invention must be totally incapable of achieving a useful result. *See Brooktree Corp. v. Advanced Micro Devices, Inc.*, 977 F.2d 1555, 1571 (Fed. Cir. 1992).

Statutory Subject Matter

A transitory, propagating signal is not statutory subject matter because it does not fall within any of the four categories of statutory subject matter. *See In re Nuijten,* 500 F.3d 1346, 1357 (Fed. Cir. 2007).

Obviousness

The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, and (3) the level of skill in the art. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). "The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 416 (2007).

ANALYSIS

Section 101 (utility) rejection of claims 1, 14-16, 31, and 32

The Examiner finds that claims 1, 14-16, 31, and 32 are all generally related to comparing two separate, imperfect samples of biometric data using a hash function to provide authentication, and that such a method could not work. Ans. 3. Appellants contend that the claimed invention could and does work for its intended purpose. App. Br. 24-34.

As best we can understand the Examiner's position, the Examiner agrees with Appellants to the extent that "the disclosure of the invention is operable," (Ans. 15), but reads the claims as covering inoperable embodiments (*id.*). Even assuming that claims must recite disclosed structure or steps to achieve utility, the Examiner does not specify what might be missing from the claims that would render the claimed invention to be operable, so as to be consistent with the "operable" invention that is disclosed.

Moreover, the statement of the rejection (Ans. 3) only goes so far as to assert that finding inputs x, x' such that $h(x)$ and $h(x')$ differ in only a small number of bits should be "hard," which does not mean impossible. Appellants have pointed to methods in the Specification that are alleged to allow the matching of inputs from consideration of hashed outputs. The rejection does not address why all, or any, of the methods are deemed not to work.

We thus agree with Appellants to the extent that the rejection fails to set forth a prima facie case for lack of utility. Contrary to the Examiner's indication (Ans. 13), Appellants were under no duty to submit amendments

or evidence in response to the § 101 rejection of claims 1, 14-16, 31, and 32 for lack of utility. We do not sustain the rejection.

Section 101 (non-statutory) rejection of claims 31-36

The Examiner finds that claims 31-36 encompass signals encoded with functional descriptive material, which do not fall within any of the categories of patentable subject matter. Ans. 3.

Appellants contend that claims 31-36 are directed to a computer readable medium tangibly embodying a program of machine readable instructions (Reply Br. 3-4); therefore, the plain language of the claims excludes "transmission media" (*id.* at 5).

Appellants' Specification (22:20 - 23:18) distinguishes signal-bearing media "tangibly embodying" a program of machine-readable instructions executable by a computer (e.g., RAM, ROM, or magnetic data storage diskette) from signal-bearing "transmission media" such as digital communication links. Because base claims 31 and 33 recite a computer-readable medium "tangibly embodying" a program of machine-readable instructions, we agree with Appellants that the claims are not directed to transitory, propagating signals. The claims are directed to functional descriptive material recorded on a computer-readable, tangible medium, which according to current Office guidelines can constitute statutory subject matter. *See* MPEP § 2106.01 (Eighth Ed., Rev. 7, Jul. 2008).

Because the Examiner's rejection is founded on an improper interpretation of the claims, we do not sustain the § 101 rejection of claims 31-36 as being directed to non-statutory subject matter.[2]

Section 103 rejection -- Borza and Kharon

Appellants submit that the Examiner has not provided sufficient reasoning for combining the teachings of Borza and Kharon. App. Br. 54-55. Appellants do not, however, show or even allege that the proffered combination would be beyond the level of ordinary skill in the art.

"[W]hen a patent 'simply arranges old elements with each performing the same function it had been known to perform' and yields no more than one would expect from such an arrangement, the combination is obvious." *KSR*, 550 U.S. at 417 (quoting *Sakraida v. Ag Pro, Inc.*, 425 U.S. 273, 282 (1976)). The operative question is "whether the improvement is more than the predictable use of prior art elements according to their established functions." *Id.*

---

[2] We are not persuaded by Appellants' mischaracterization (App. Br. 44) of *In re Beauregard*, 53 F.3d 1583 (Fed. Cir. 1995), as having "upheld" a computer program as patentable subject matter "because it was claimed in terms of an article of manufacture as contained on a floppy disk." *Beauregard* was merely an order remanding a proceeding to the USPTO because the parties agreed that the printed matter doctrine did not apply, based on the Office position that computer programs embodied in a tangible medium were patentable subject matter under § 101. Appellants' reference to claims in a U.S. Patent (Reply Br. 4) that has an inventive entity different from that in the *Beauregard* case is also unhelpful.

We are therefore not persuaded by Appellants' general allegations of a lack of motivation to combine, and turn to consider the features that Appellants argue to be missing from the prior art.

Section 103 rejection of claims 1, 9, 11-23, 29, 30, and 33-36

Appellants contend that the Examiner is incorrect in finding that Borza teaches, as recited in claim 1, "to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P." App. Br. 49, 52-53, 56-57.

According to Appellants, the argued claim 1 recitation is described in the Specification at page 13, lines 13 through 17 and page 14, lines 3 through 4 and 12 through 15. App. Br. 5 ("Summary of The Claimed Subject Matter").

We reproduce the referenced text of the Specification below.

> It is noted that *P* cannot be extracted from *h*(*P*) since *h* is a secure hash function, and thus the inverse of *h* is either impossible or hard to compute and if some *P'* must be matched to the *P*s (*e.g.*, in the investigation of a crime), one compares *h*(*P'*) preferably to all available *h*(*P*)s to check if one of them matches. This is illustrated in Fig. 2.

Spec. 13:13-17.

> In step 204 [Fig. 2], *h*(*P'*) is compared against *h*(*P*) stored in a database 205, to determine whether there is a match.

Id. at 14:3-4.

> *P* cannot be extracted from *h*(*P*), except by the trusted party if some such party has been designated to receive *K*. If

> some *P′* is observed (e.g., in the investigation of a crime or the like), one compares *h*(*P′*) to all available *h*(*P*)s to determine if one of them matches.

Id. at 14:12-15.

The Specification sections referenced by Appellants describe comparing h(P') to available h(P)s to determine if there is a match. The Specification does not describe determining whether P' is close to a predetermined subject by comparing h(P') to available h(P)s to determine whether P' "substantially matches, but does not exactly match," one of said data set P, at least not in the section purported by Appellants to describe the invention now claimed. However, the Examiner has found, implicitly, that the disclosure somewhere supports the language of claim 1 -- a Section 112 rejection is not before us.

In any event, the sections of Borza relied on by the Examiner (Ans. 4), to show the claim 1 recitation in controversy, teach comparing encrypted biometric information against an encrypted template (FF 1) and comparing unencrypted information against unencrypted templates (FF 2-4). The Examiner has not provided a satisfactory explanation as to how these sections of Borza might teach determining "whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P," as recited in claim 1.

The Examiner further finds that Borza does not teach encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability. Ans. 6. The Examiner relies on Kharon to teach this limitation. *Id.*

However, the section of Kharon relied on by the Examiner does not appear to teach encrypting a predetermined number of such sub-collections as required by claim 1. *See* FF 5. The Answer (at 18) responds to Appellants' argument (App. Br. 50) about Kharon not describing the extraction of multiple subsets, but seems to ignore Appellants' argument with respect to the lack of encrypting the subsets, which is also set out at page 50 of the Appeal Brief.

Similarly, in the rejection of claims 9, 15, 17, 19, 29, 33, and 35, the Examiner relies on Kharon to teach encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability. Final Rejection 13-17, Ans. 10. However, the section of Kharon relied on by the Examiner has not been shown to teach encrypting a predetermined number of such sub-collections as required by claims 9, 15, 17, 19, 29, 33, and 35.

In view of the claim dependencies, we are thus persuaded of error in the § 103(a) rejection of claims 1, 9, 11-23, 29, 30, and 33-36.

Section 103 rejection of claims 5-8, 24-28, 31, and 32

Appellants contend that Borza does not disclose or suggest "to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P" as recited in claim 1. App. Br. 49. Appellants further contend that claims 5, 24, 27, and 31 are patentable "for the same reasons" as claim 1, because each recites "somewhat similar" features. *Id.*

Independent claim 5 does not require comparing anything to anything. Independent claims 24 and 31 recite comparing h(P') to available h(P)s to determine whether data set P' is "close to" some data set P. Independent claim 27 recites comparing an encrypted data set of a data set P' to at least one encrypted data set of data set P to determine whether there "is a match" and to determine whether the data set P' is a predetermined subject.

We find that claims 5, 24, 27, and 31 do not recite the features of claim 1 that are argued by Appellants as distinguishing over the applied prior art. Appellants have not demonstrated error in the rejection of independent claims 5, 24, 27, and 31. In view of claims depending from the independent claims, Appellants have failed to show error in the rejection of claims 5-8, 24-28, 31, and 32. *See* 37 C.F.R. § 41.37(c)(1)(vii).

CONCLUSIONS OF LAW

(1) Appellants have shown that the Examiner erred in finding that the invention recited in claims 1, 14-16, 31, and 32 lacks utility.

(2) Appellants have shown that the Examiner erred in finding that claims 31-36 are directed to a transitory, propagating signal.

(3) Appellants have shown that the Examiner erred in finding that the combination of Borza and Kharon teaches "to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P" and "encrypting a predetermined number of such sub-collections" as recited in claim 1.

DECISION

The rejection of claims 1, 14-16, 31, and 32 under 35 U.S.C. § 101 as lacking utility is reversed.

The rejection of claims 31-36 under 35 U.S.C. § 101 as being directed to non-statutory subject matter is reversed.

The rejection of claims 1, 9, 11-23, 29, 30, and 33-36 under 35 U.S.C. § 103(a) as being unpatentable over Borza and Kharon is reversed.

The rejection of claims 5-8, 24-28, 31, and 32 under 35 U.S.C. § 103(a) as being unpatentable over Borza and Kharon is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 41.50(f).

AFFIRMED-IN-PART

msc

MCGINN INTELLECTUAL PROPERTY LAW GROUP, PLLC
8321 OLD COURTHOUSE ROAD
SUITE 200
VIENNA VA 22182-3817